PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

YAO *et al.*

Serial No.: Pending

Filed: June 19, 2003

For: METHOD FOR PREVENTING IP ADDRESS CHEATING IN DYNAMIC ADDRESS ALLOCATION

: Office of Initial Patent Examination

COMPLETION OF CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants hereby submit the official certified copy of priority document number 02125007.3 in connection with the above identified application, benefit of which is claimed in the declaration of this application. The Examiner is most respectfully requested to acknowledge receipt of this certified copy in the next Official Action.

Respectfully submitted,

BACON & THOMAS, PLLC

By: Richard E. Fichter

Richard E. Fichter
Registration No. 26,382

625 Slaters Lane, 4th Fl.
Alexandria, Virginia 22314
Phone: (703) 683-0500
Facsimile: (703) 683-1080

REF:kdd
Completion of Claim for Priority.wpd

June 19, 2003

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2002 06 22

申　请　号：　02 1 25007.3

申请类别：　发明

发明创造名称：　一种动态地址分配中防止ＩＰ地址欺骗的方法

申　请　人：　华为技术有限公司

发明人或设计人：姚析；修亦宏；潘凝

中华人民共和国
国家知识产权局局长　王景川

2002 年 12 月 9 日

权 利 要 求 书

1、一种动态地址分配中防止 IP 地址欺骗的方法，其特征在于包括：

（1）用户终端向交换机发出 ARP 报文；

（2）交换机对 ARP 报文中的源 MAC 地址和源 IP 地址进行检查，即在合法用户地址表中查找是否存在匹配项，如果存在，将用户终端发出的 ARP 报文的源 IP 地址和源 MAC 地址加入 ARP 表，从而使用户终端能够上网通信；否则，丢弃该报文。

2、根据权利要求 1 所述的动态地址分配中防止 IP 地址欺骗的方法，其特征在于，还包括在所述的合法用户地址表中增加一个新的用户终端的信息，具体经过以下步骤：

（21）用户终端通过 DHCP 中继向 DHCP 服务器发出 DHCPDISCOVER 报文；

（22）DHCP 服务器通过 DHCP 中继向用户终端发出 DHCPOFFER 响应报文；

（23）用户终端通过 DHCP 中继向 DHCP 服务器发送 DHCPREQUEST 报文；

（24）DHCP 中继收到 DHCP 服务器的 DHCPACK 响应报文；

（25）交换机搜索已存在的合法用户地址表，如果 IP 地址被设置为静态表项，则进行步骤（26），否则，进行步骤（27）；

（26）向 DHCP 服务器发送 DHCPDECLINE 报文，标记此 IP 地址为已分配，同时，向用户终端发送 DHCPNAK 报文，通知其申请其他 IP 地址，

然后转入步骤（21），继续申请 IP 地址；

（27）交换机进行转发处理，并把分配给用户的 IP 地址和 MAC 地址写入合法用户地址表。

3、根据权利要求 2 所述的动态地址分配中防止 IP 地址欺骗的方法，其特征在于，所述静态表项是固定 IP 地址的用户终端的信息。

4、根据权利要求 3 所述的动态地址分配中防止 IP 地址欺骗的方法，其特征在于，所述静态表项根据固定 IP 地址的用户终端的实际使用情况进行添加和删除。

5、根据权利要求 4 所述的动态地址分配中防止 IP 地址欺骗的方法，其特征在于，所述静态表项的添加和删除是通过命令行或网管手工配置的。

6、根据权利要求 4 或 5 所述的动态地址分配中防止 IP 地址欺骗的方法，其特征在于，所述静态表项的信息删除时，交换机的处理步骤为：

（61）交换机向服务器发送 DHCPREQUST 请求报文，去掉步骤（26）中对此 IP 地址所做的标记；

（62）交换机向服务器发送 DHCPRELEASE 报文，释放 IP 地址，使其能够被动态分配给用户。

说 明 书

一种动态地址分配中防止IP地址欺骗的方法

技术领域

本发明涉及通讯网络的接入方法，具体涉及宽带网络中动态地址的分配方法。

背景技术

随着网络规模的不断扩大、网络复杂度的不断提高，进行网络配置也变得越来越复杂，因此产生了DHCP协议（动态主机配置协议，Dynamic Host Configuration Protocol）并得到了广泛应用。DHCP是在BOOTP（引导协议，Bootstrap Protocol）基础上产生的，增加了动态分配的能力，即DHCP给接入用户终端指定一个有时间限制的IP地址，到时间或该用户终端明确表示放弃这个地址时，这个地址可以被其它用户使用，从而提高了资源利用率。在给一个临时连入网络的用户终端分配地址或者在一组不需要永久IP地址的用户终端中共享一组有限的IP地址时，可以利用动态分配；当一个新用户终端要永久的接入一个网络时，而网络的IP地址非常有限，为了将来这个用户不再需要永久接入时能回收IP地址，也可以利用动态分配。

图1为实际组网应用情况，包括具有DHCP中继功能的三层交换机，与其相连的一个网段中的主、备DHCP服务器，另一个网段中的DHCP客户。

DHCP动态分配是通过服务器和用户终端之间的DHCP报文交互完成的，而DHCP报文是广播报文，不能跨越网段，这样DHCP服务器只能为

本网段的用户终端提供服务。但是由于资源限制，不可能为每个网段都配置一台DHCP服务器，而且出于安全性考虑，DHCP服务器通常都是处于一个单独的网段。这样就需要DHCP服务器可以为不在其网段的用户终端提供服务。而DHCP中继为DHCP广播报文提供网段间的转发功能，使得DHCP服务器实现为不在其网段的用户终端提供服务。

但在使用DHCP动态分配方式的网络中，有一些用户终端不通过DHCP中继正常获取IP地址，而是非法设置分配给其他用户的IP地址上网。对于这种IP地址欺骗问题，目前是通过用户终端计算机系统引导时发出的免费ARP报文来检查的，如果有非法用户终端占用了自己的IP地址，用户终端计算机就会报告地址冲突。但是这样通过计算机自身检测冲突并不能从根本上解决问题，非法用户还是可以通过IP地址欺骗上网。

发明内容

本发明的目的在于提供一种在动态地址分配中防止 IP 地址欺骗问题的方法，从根本上解决了 IP 地址盗用的问题，使利用 IP 地址欺骗方法上网的非法用户，不能够上网通信，从而保护合法用户的正常使用。

为达到上述目的，本发明采用如下步骤：

（1）用户终端向交换机发出 ARP（地址解析协议）请求或响应报文；

（2）交换机对 ARP 报文中的源 MAC（网卡硬件地址）地址和源 IP 地址进行检查，即在合法用户地址表中查找是否存在匹配项，如果存在，按正常流程处理，即将用户终端发出的 ARP 报文的源 IP 地址和源 MAC 地址加入 ARP 表，从而使用户终端能够上网通信；否则，丢弃该报文。

在合法用户地址表中增加一个新的用户终端的信息经过以下步骤：

（21）用户终端通过 DHCP 中继向 DHCP 服务器发出 DHCPDISCOVER 报文；

（22）DHCP 服务器通过 DHCP 中继向用户终端发出 DHCPOFFER 响应报文；

（23）用户终端通过 DHCP 中继向 DHCP 服务器发送 DHCPREQUEST 报文；

（24）DHCP 中继收到 DHCP 服务器的 DHCPACK 响应报文；

（25）交换机搜索已存在的合法用户地址表，如果 IP 地址被设置为静态表项，则进行步骤（26），否则，进行步骤（27）；

（26）向 DHCP 服务器发送 DHCPDECLINE 报文，标记此 IP 地址为已分配，同时，向用户终端发送 DHCPNAK 报文，通知其申请其他 IP 地址，然后转入步骤（21），继续申请 IP 地址；

（27）交换机进行转发处理，并把分配给用户的 IP 地址和 MAC 地址写入合法用户地址表。

上述步骤中，静态表项是固定 IP 地址的用户终端的信息，它是根据固定 IP 地址的用户终端的实际使用情况进行添加和删除的，可以通过命令行或网管手工配置，删除时交换机的处理步骤为：

交换机向服务器发送 DHCPREQUST 请求报文，去掉步骤（26）中对此 IP 地址所做的标记；交换机向服务器发送 DHCPRELEASE 报文，释放 IP 地址，使其能够被动态分配给用户。

本发明对用户终端的 ARP 报文进行合法地址的检查，如果在合法用户地址表中没有匹配项即丢弃该报文，使利用 IP 地址欺骗的非法用户不能

进行网上通信，并且合法用户的可以继续正常使用，不会受到影响，从而在根本上解决了问题。

对于固定 IP 地址的用户终端，采用向合法用户地址表手工配置静态表项的方法。当新的用户终端请求分配 IP 地址时，判断该地址是否在静态表项中，如果在，则通知该用户申请其他 IP 地址，这样保证了已经分配给固定用户终端的 IP 地址不会再分配给其他用户终端使用，从而避免了由于 IP 地址被重新分配而引起的合法固定 IP 用户终端无法上网的问题。

下面将结合附图及实施例对本发明作进一步说明。

附图说明

图1为本发明的网络应用环境示意图；

图2为本发明的实施方案流程图；

图3为在合法用户地址表中建立一个新用户信息的流程图。

具体实施方式

如附图 2 所示，在动态地址分配中防止 IP 地址欺骗的处理步骤为：

步骤 1：用户终端向交换机发出 ARP 报文，该报文中携带该用户终端的 MAC 地址和 IP 地址，ARP 报文包括请求或响应报文；

步骤 2：交换机对 ARP 报文中的源 MAC 地址和源 IP 地址进行检查，即在合法用户地址表中查找是否存在匹配项，如果存在，则表明此用户终端是通过 DHCP 中继合法获得的 IP 地址，按正常流程处理，即将用户终端发出的 ARP 报文的源 IP 地址和源 MAC 地址加入 ARP 表，从而使用户终端能够上网通信；如果不存在匹配项，则表明此用户使用的是非法获得的

IP 地址，丢弃该报文，不生成相应的 ARP 的表项，这样进行 IP 地址欺骗的非法用户就无法上网通信了。

如图 3 所示，在合法用户地址表中增加一个新的用户终端的信息经过以下步骤：

步骤 21：用户终端通过 DHCP 中继向 DHCP 服务器发出 DHCPDISCOVER 报文，要求 DHCP 服务器提供服务；

步骤 22：DHCP 服务器通过 DHCP 中继向用户发出 DHCPOFFER 响应报文，向用户表明可以提供服务；

步骤 23：用户终端通过 DHCP 中继向 DHCP 服务器发送 DHCPREQUEST，报文申请 IP 地址；

步骤 24：DHCP 中继收到 DHCP 服务器的 DHCPACK 响应报文，报文中有分配给用户的 IP 地址、掩码以及一些其它配置信息如网关地址等；

步骤 25：交换机搜索已存在的合法用户地址表，如果 IP 地址被设置为静态表项，则进行步骤（26），否则，进行步骤（27）；

步骤 26：向 DHCP 服务器发送 DHCPDECLINE 报文，标记此 IP 地址为已分配，并向用户终端发送 DHCPNAK 报文，通知其申请其他 IP 地址，然后转入步骤（21），继续申请 IP 地址；

步骤 27：交换机进行转发处理，并把分配给用户的 IP 地址和 MAC 地址写入合法用户地址表。

下面详细介绍前面所述的静态表项的情况：

有些用户终端需要设置固定的 IP 地址，而固定 IP 地址不是通过 DHCP 报文获得 IP 地址的，因此合法地址表中不存在其对应的表项，为了使其

能够通过地址检查正常上网，采用在合法用户地址表中设置静态表项的方法，静态表项为固定 IP 地址的用户终端的信息，它根据固定 IP 地址的用户终端的实际使用情况进行添加和删除，可以通过命令行或网管手工配置。如步骤 24、25、26 所述，当 DHCP 中继收到 DHCP 服务器的 DHCPACK 响应报文时，交换机搜索合法用户地址表，如果此 IP 地址被设置为静态表项，则向 DHCP 服务器发送 DHCPDECLINE 报文，标记此 IP 地址为已分配，使其不会再被 DHCP 服务器分配给其他用户终端，同时，向用户终端发送 DHCPNAK 报文，通知其申请其他 IP 地址。

当某个固定 IP 用户终端不再需要固定的 IP 地址时，手工删除静态表项，这时交换机会向服务器发送 DHCPREQUST 请求报文和 DHCPRELEASE 报文，除去此 IP 地址的已分配标记，从而使其能够继续被 DHCP 服务器提供给其他用户终端使用。

说 明 书 附 图

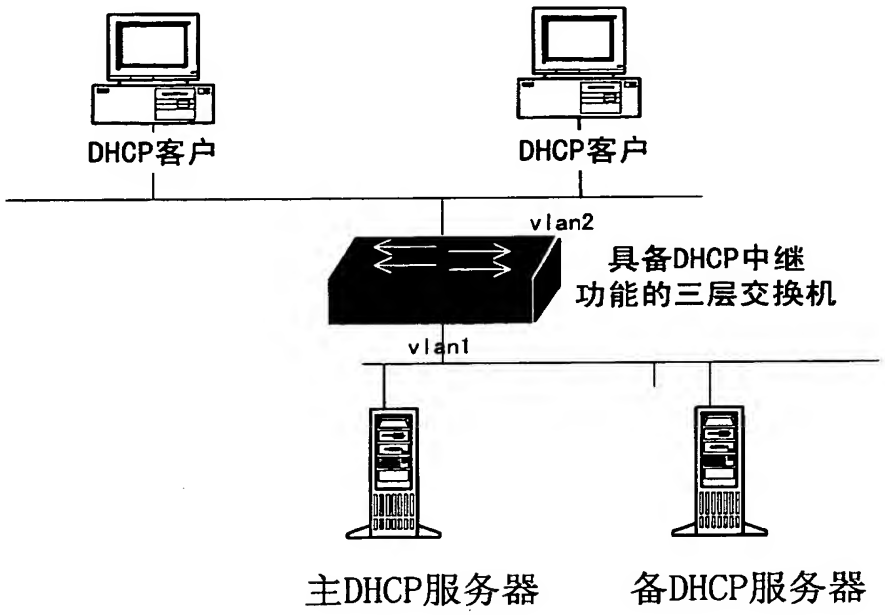
DHCP客户
DHCP客户
vlan2
具备DHCP中继
功能的三层交换机
vlan1
主DHCP服务器
备DHCP服务器

图 1

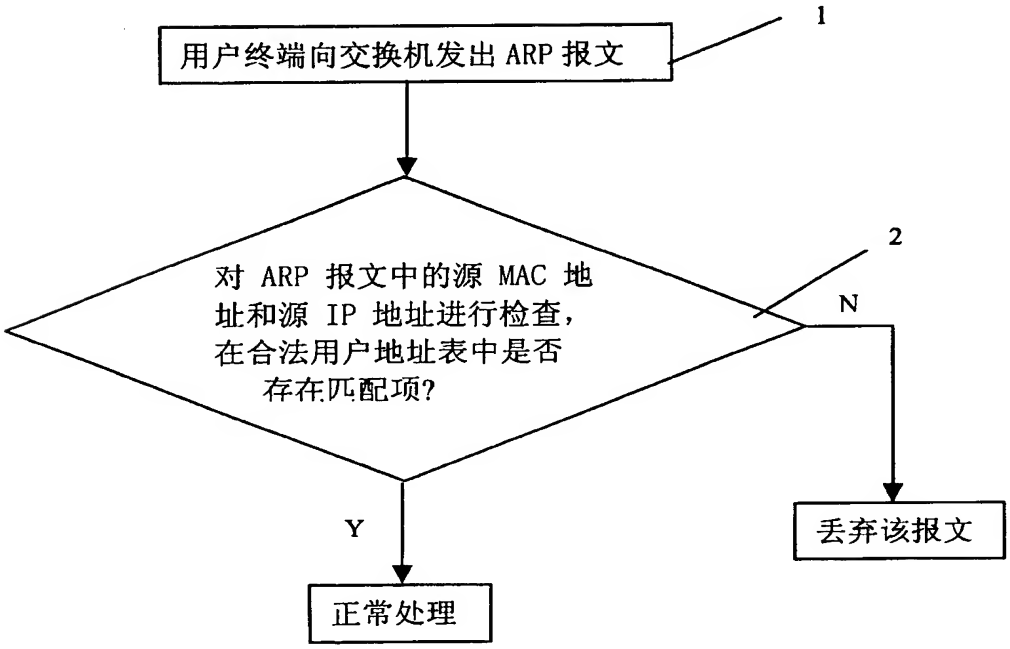
1
用户终端向交换机发出 ARP 报文
2
对 ARP 报文中的源 MAC 地址和源 IP 地址进行检查，在合法用户地址表中是否存在匹配项?
N
Y
丢弃该报文
正常处理

图 2

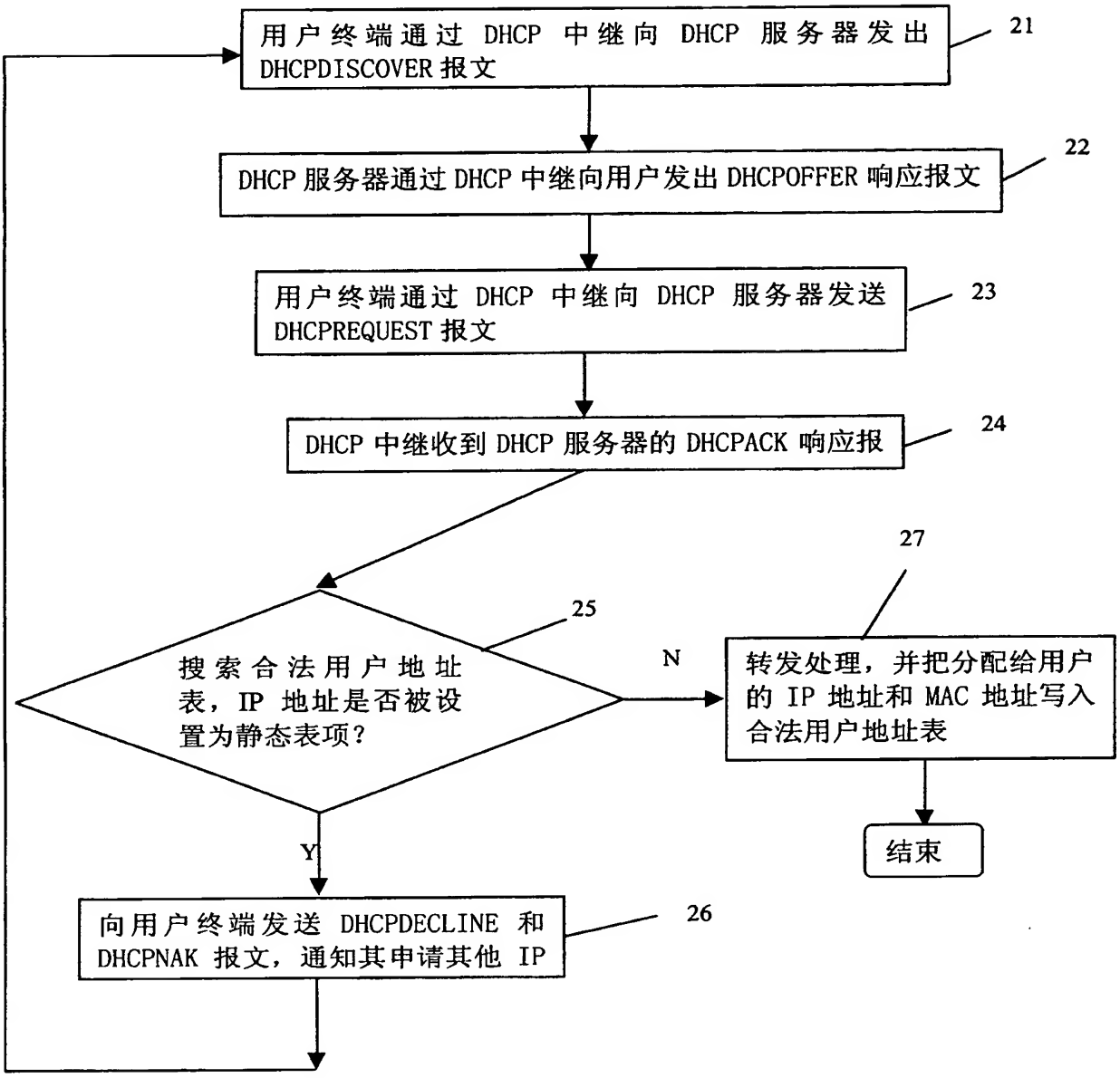
用户终端通过 DHCP 中继向 DHCP 服务器发出 DHCPDISCOVER 报文
21
DHCP 服务器通过 DHCP 中继向用户发出 DHCPOFFER 响应报文
22
用户终端通过 DHCP 中继向 DHCP 服务器发送 DHCPREQUEST 报文
23
DHCP 中继收到 DHCP 服务器的 DHCPACK 响应报
24
搜索合法用户地址表，IP 地址是否被设置为静态表项？
25
N
Y
转发处理，并把分配给用户的 IP 地址和 MAC 地址写入合法用户地址表
27
结束
向用户终端发送 DHCPDECLINE 和 DHCPNAK 报文，通知其申请其他 IP
26

图 3